PGCD – Bézout - Gauss.

Corrigés d'exercices

Les exercices du livre corrigés dans ce document sont les suivants :

N°78 page 500

Notons que dans cet exercice la formulation du petit théorème de Fermat est quelque peu différente de celle de l'exercice N°12 de la page 485. Ceci dit, les deux formulations sont équivalentes ! Lorsque p est premier, « *a* entier premier avec *p* » équivaut à « *p* ne divise pas *a* ».

1. On suppose donc ici que l'on a : $n = p_1 \times p_2 \times ... \times p_k$ $(k \geq 2)$ où les p_i sont des entiers premiers deux à deux distincts tels que $\forall i \in \llbracket 1 ; k \rrbracket, (p_i - 1) | (n-1)$.
Comme on a $k \geq 2$, le produit $p_1 \times p_2 \times ... \times p_k$ (qui correspond à la décomposition en facteurs premiers de *n*) comporte au moins deux facteurs distincts. L'entier *n* admet donc des diviseurs différents de 1 et de lui-même. Il n'est donc pas premier.

L'entier *n* n'est pas premier.

2. **a.** L'entier *a* est supposé premier avec *n*.
Si un p_i divisait *a*, il serait diviseur commun (différent de 1 puisque p_i est premier) de *a* et *p*, ce qui est absurde et contredit l'hypothèse ci-dessus.
Ainsi :

$\forall i \in \llbracket 1 ; k \rrbracket, p_i \nmid a$

b. Pour tout entier naturel *i* dans $\llbracket 1 ; k \rrbracket$, p_i est premier et ne divise pas *a*. D'après le petit théorème de Fermat, on a donc : $a^{p_i - 1} \equiv 1 (p_i)$.

$\forall i \in \llbracket 1 ; k \rrbracket, a^{p_i - 1} \equiv 1 (p_i)$

c. D'après la question précédente, on a : $\forall i \in \llbracket 1;k \rrbracket, a^{p_i-1} \equiv 1(p_i)$.

On sait également, par hypothèse, que $\forall i \in \llbracket 1;k \rrbracket, (p_i-1) \mid (n-1)$. Ainsi, pour tout entier i dans $\llbracket 1;k \rrbracket$, il existe un entier naturel k_i tel que $n-1 = k_i(p_i-1)$.

Il vient alors : $a^{p_i-1} \equiv 1(p_i) \Rightarrow \left(a^{p_i-1}\right)^{k_i} \equiv 1^{k_i}(p_i) \Leftrightarrow a^{k_i(p_i-1)} \equiv 1(p_i) \Leftrightarrow a^{n-1} \equiv 1(p_i)$.

$\forall i \in \llbracket 1;k \rrbracket, a^{n-1} \equiv 1(p_i)$

3. **a.** On utilise ici le résultat général (cf. exercice N°77 page 500) : si des nombres premiers, deux à deux distincts, divisent individuellement un entier donné alors leur produit divise également cet entier.
D'après la question précédente, chaque p_i divise $a^{n-1}-1$ et on en déduit que leur produit, c'est-à-dire *n*, divise également $a^{n-1}-1$: $n \mid (a^{n-1}-1)$. D'où : $a^{n-1} \equiv 1(n)$

$a^{n-1} \equiv 1(n)$

b. Rappelons que l'hypothèse « *a* premier avec *n* » avait été faite. Ainsi, pour tout entier a premier avec n, on a (cf. question précédente) : $a^{n-1} \equiv 1(n)$. Par définition d'un nombre de Carmichaël :

L'entier *n* est un nombre de Carmichaël.

4. On a facilement : $n = 561 = 3 \times 11 \times 17$. On peut poser : $p_1 = 3$, $p_2 = 11$ et $p_3 = 17$.
On a alors :

$$n-1 = 560 = 2 \times 280 = (p_1-1) \times 280$$
$$n-1 = 560 = 10 \times 56 = (p_2-1) \times 56$$
$$n-1 = 560 = 16 \times 35 = (p_3-1) \times 35$$

Ainsi, 561 est le produit de trois nombres premiers $p_1 = 3$, $p_2 = 11$ et $p_3 = 17$ tels que p_1-1, p_2-1 et p_3-1 divisent $n-1$.
D'après les questions traitées précédemment, 561 est un nombre de Carmichaël.

561 est un nombre de Carmichaël.

N°82 page 501

1. **a.** On a facilement :

$$\begin{aligned} 2\,017 &= 123\times 16 + 49 \\ 123 &= 49\times 2 + 25 \\ 49 &= 25\times 1 + 24 \\ 25 &= 24\times 1 + 1 \end{aligned}$$

On multiplie alors classiquement chaque ligne à partir de la dernière par un coefficient entier approprié :

$$\begin{aligned} 2\,017 &= 123\times 16 + 49 && \times(-1) \\ 123 &= 49\times 2 + 25 && \times 2 \\ 49 &= 25\times 1 + 24 && \times(-1) \\ 25 &= 24\times 1 + 1 \end{aligned}$$

En additionnant alors membre à membre les quatre égalités ainsi obtenues, on obtient :

$$\begin{aligned} &-5\times 2\,017 + 2\times 123 + \cancel{(-1)\times 49} + \cancel{25} \\ &\quad = (-80)\times 123 + \cancel{(-5)\times 49} + \cancel{4\times 49} + \cancel{2\times 25} + \cancel{(-1)\times 25} + \cancel{(-1)\times 24} + \cancel{1\times 24} + 1 \\ &\Leftrightarrow -5\times 2\,017 + 2\times 123 = (-80)\times 123 + 1 \\ &\Leftrightarrow 82\times 123 + (-5)\times 2\,017 = 1 \end{aligned}$$

Finalement :

Pour $(u, v) = (82, -5)$, on a : $123u + 2\,017v = 1$.

b. Comme $82\times 123 + (-5)\times 2\,017 = 1$, il vient immédiatement : $123\times 82 \equiv 1\,(2\,017)$.

Pour $k = 82$, on a : $123k \equiv 1\,(2\,017)$.

c. Soit x un entier quelconque tel que : $123x \equiv 456\,(2\,017)$.

Il en découle : $123x \times k \equiv 456 \times k\,(2\,017)$.

Comme $123k \equiv 1\,(2\,017)$, il vient aussi $123k \times x \equiv 1 \times x\,(2\,017)$.

De $123kx \equiv 456k\,(2\,017)$ et $123kx \equiv x\,(2\,017)$, il découle alors : $456k \equiv x\,(2\,017)$.

Ainsi, pour tout entier x : $123x \equiv 456\,(2\,017) \Rightarrow 456k \equiv x\,(2\,017)$

Réciproquement, soit x un entier tel que $x \equiv 456k\ (2\,017)$ où $123k \equiv 1\,(2\,017)$.
Il en découle : $x \times 123 \equiv 456k \times 123\,(2\,017)$.
Comme $123k \equiv 1\,(2\,017)$, il vient aussi $123k \times 456 \equiv 1 \times 456\,(2\,017)$.
De $456k \times 123 \equiv 123x\,(2\,017)$ et $123k \times 456 \equiv 456\,(2\,017)$, il découle alors :
$123x \equiv 456\,(2\,017)$.

Ainsi, pour tout entier x : $\underline{x \equiv 456k\ (2\,017) \Rightarrow 123x \equiv 456\,(2\,017)}$

Finalement :

$$\forall x \in \mathbb{Z}, 123x \equiv 456\,(2\,017) \Leftrightarrow 456k \equiv x\,(2\,017)$$
où k est un entier tel que $123k \equiv 1\,(2\,017)$.

d. D'après la question précédente, résoudre $123x \equiv 456\,(2\,017)$ équivaut à résoudre $456k \equiv x\,(2\,017)$ avec $123k \equiv 1\,(2\,017)$. Or $456k \equiv x\,(2\,017)$ signifie qu'il existe un entier k' tel que $456k + 2\,017k' = x$. Dans cette égalité, on peut choisir n'importe quel entier k tel que $123k \equiv 1\,(2\,017)$. L'entier 82 (cf. la question 1.b.) convient.
Ainsi :

$$\begin{aligned} x &= 456 \times 82 + 2\,017k' = 37\,392 + 2\,017k' \\ &= 2\,017 \times 18 + 1\,086 + 2\,017k' \\ &= 1\,086 + 2\,017 \times (18 + k') \end{aligned} \quad .$$

Lorsque k' parcourt $\mathbb{Z}$, il en va de même pour $18 + k'$. Les solutions de $456k \equiv x\,(2\,017)$ sont les entiers de la forme $x = 1\,086 + 2\,017K$ où K est un entier quelconque.

Les solutions de $123x \equiv 456\,(2\,017)$ sont les entiers de la forme
$x = 1\,086 + 2\,017K$
où K est un entier quelconque.

e. L'entier naturel n cherché est solution de $123x \equiv 456\,(2\,017)$. D'après la question précédente, il est de la forme $1\,086 + 2\,017K$. Il est non nul puisque l'équation $1\,086 + 2\,017n = 0$ n'admet pas de solution entière.
On a alors : $1 \leq n \leq 2\,016 \Leftrightarrow 1 \leq 1\,086 + 2\,017K \leq 2\,016 \Leftrightarrow -1\,085 \leq 2\,017K \leq 930$.
On en déduit, K étant entier : $K = 0$ puis $n = 1\,086 + 2\,017K = 1\,086$.

Le seul entier naturel compris entre 1 et 2 017 et vérifiant $123n \equiv 456\,(2\,017)$ est 2 016.

2. **a.** Comme l'entier naturel *a* est strictement inférieur à 2 017, tout diviseur commun positif de 2 017 et *a* est strictement inférieur à 2 017. Or, 2 017 étant premier, son seul diviseur positif qui lui est strictement inférieur est 1.
On en déduit finalement que le seul diviseur positif commun à *a* et 2 017 est 1 :

$$\text{PGCD}(a, 2\,017) = 1$$

On en déduit, d'après le théorème de Bézout, qu'il existe deux entiers *m* et *n* tels que : $am + 2\,017n = 1$, d'où $am \equiv 1\,(2\,017)$.

Il existe un entier *m* tel que $am \equiv 1\,(2\,017)$.

b. Dans cette question, nous allons reprendre, en la généralisant, la démarche de la question 1.
On s'intéresse ici à l'équation $ax \equiv b\,(2\,017)$ comme généralisation de l'équation $123x \equiv 456\,(2\,017)$.
En reprenant la démarche de la question 1.c., on obtient :

- Soit *x* un entier quelconque tel que : $ax \equiv b\,(2\,017)$.
  Il en découle : $ax \times m \equiv b \times m\,(2\,017)$.
  Comme $am \equiv 1\,(2\,017)$, il vient aussi $am \times x \equiv 1 \times x\,(2\,017)$.
  De $ax \times m \equiv b \times m\,(2\,017)$ et $am \times x \equiv x\,(2\,017)$, il découle alors : $bm \equiv x\,(2\,017)$.

  Ainsi, pour tout entier *x* : $ax \equiv b\,(2\,017) \Rightarrow bm \equiv x\,(2\,017)$

- Réciproquement, soit *x* un entier tel que $bm \equiv x\,(2\,017)$ où $am \equiv 1\,(2\,017)$.
  Il en découle : $a \times bm \equiv a \times x\,(2\,017)$.
  Comme $am \equiv 1\,(2\,017)$, il vient aussi $am \times b \equiv 1 \times b\,(2\,017)$.
  De $a \times bm \equiv ax\,(2\,017)$ et $am \times b \equiv b\,(2\,017)$, il découle alors : $ax \equiv b\,(2\,017)$.

  Ainsi, pour tout entier *x* : $bm \equiv x\,(2\,017) \Rightarrow ax \equiv b\,(2\,017)$

Finalement, on a l'équivalence :

$$ax \equiv b\,(2\,017) \Leftrightarrow bm \equiv x\,(2\,017)$$

Résoudre $ax \equiv b\,(2\,017)$ équivaut donc à résoudre $bm \equiv x\,(2\,017)$.
L'entier x est solution de $bm \equiv x\,(2\,017)$ si, et seulement si, il existe un entier *k* tel que $x = bm + 2\,017k$.

Ainsi :

> Les solutions de $ax \equiv b\,(2\,017)$ sont les entiers de la forme $x = bm + 2\,017k$
> où m est un entier tel que $am \equiv 1\,(2\,017)$.

Effectuons enfin la division euclidienne de bm par 2 017 : $bm = 2\,017q + r$ avec $0 \leq r \leq 2\,016$. Les solutions de $ax \equiv b\,(2\,017)$ sont donc les entiers de la forme :

$$x = 2\,017q + r + 2\,017k = 2\,017(q+k) + r = 2\,017K + r \text{ avec } 0 \leq r \leq 2\,016$$

Ainsi : $0 \leq x \leq 2\,016 \Leftrightarrow 0 \leq 2\,017K + r \leq 2\,016 \Leftrightarrow -r \leq 2\,017K \leq 2\,016 - r$.
Comme $0 \leq r \leq 2\,016$, on a :

$$-r \leq 2\,017K \leq 2\,016 - r \Rightarrow -2\,016 \leq -r \leq 2\,017K \leq 2\,016 - r \leq 2\,016$$

Le seul multiple de 2 017 compris entre $-2\,016$ et 2 016 étant 0, il existe donc une unique valeur de K telle que $x = 2\,017K + r$ soit compris entre 0 et 2 016.

Finalement :

> Pour tout entier b, il existe un unique entier x vérifiant :
> $0 \leq x \leq 2\,016$
> $ax \equiv b\,(2\,017)$